UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/585,517	07/10/2006	Saar Wilf	2043.561US1	7666

49845 7590 08/10/2011

SCHWEGMAN, LUNDBERG & WOESSNER/EBAY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
MACILWINEN, JOHN MOORE JAIN	
ART UNIT	PAPER NUMBER
2442	

NOTIFICATION DATE	DELIVERY MODE
08/10/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO@SLWIP.COM
request@slwip.com

Office Action Summary	Application No.	Applicant(s)	
	10/585,517	WILF ET AL.	
	Examiner	Art Unit	
	JOHN MACILWINEN	2442	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/21/2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7,9-39,41,43,44 and 46-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7,9-39,41,43,44 and 46-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/1/2010,11/22/2010,1/21/2011*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 09/01/2010 have been fully considered but they are not persuasive.

2. On page 17, continuing through page 18, Applicant argues that in Pazi (US 2003/0110274 A1),

> "*a TTL entry is an expected characteristic of a packet and* ***not a "feature of an original source" of a first information element*** *or a* ***"feature of the potential relay device."***

Pazi's stored "TTL entry" corresponds to the claimed "identifying feature of an original source of said first information element"; i.e., a database of stored "expected", "reference", "proper TTL value[s]" (*Pazi, [7,9,15,30]*). These stored authenticated, reference TTL values are paired with an IP source address (*Pazi, [47]*). This reference TTL value pairing corresponds to a "feature of the original source", where the "original source" is represented by the IP source address with which the TTL value is stored. As Applicant quotes on page 17, Pazi notes that a TTL value is

> "*the number of hops that a packet has travelled through the network since leaving its source".*

Thus a TTL value of a packet is based on the source of the packet and thus meets the claim limitations as being a "feature of the original source", particularly when the TTL value in question corresponds to the stored database reference, authentic TTL values.

The “feature of the potential device” corresponds to the TTL value of a presently intercepted packet; i.e., *Pazi, [30]* describing that

> “*The guard device compares the IP source address and TTL field of each packet that it intercepts against reference values.*"

As Pazi further elaborates in [67-68], packets that are from their authentic, original source contain a TTL value that corresponds to the expected, authentic value stored in the TTL/IP address database discussed in the preceding paragraphs. If a packet does not contain a TTL value that corresponds to the TTL value stored in the database, then the packet is considered to be “spoofed” as it lacks the authenticated "feature of the original source".

Applicant’s arguments thus are not persuasive.

3. On page 18, Applicant addresses Mackay.

> “*Mackay simply discusses methods an internet service provider (ISP can use to detect if a user is using proxy services.”*

including detecting if

> “*the user is behind a NAT*”

Proxy services and NATs, as Applicant notes in their Specification on page 14, lines 27 - 30, however, correspond to types of the claimed relay devices. As the 06/01/2010 Final Rejection noted, Mackay was relied upon for teaching determining relay devices. The Examiner thus maintains his reliance upon the teachings of Mackay as previously cited.

4. Continuing on page 18, Applicant argues that

> "*A **TTL value** **of a spoofed packet** not being from the same source is not the same as **a packet** not from the same source.*"

Applicant's argument appears to correspond with those addressed above. Pazi teaches utilizing a TTL value to determine if a packet's claimed source has been "spoofed"; i.e., that the packet is not actually from the source it claims.

As noted above, a TTL value is based on a packets source, and is used by Pazi in view of Mackay as an indicator used for validation of the source of a packet.

Pazi in view of Mackay use variances in TTL values as indicators that packets are from a relay device, such as a NAT, rather than the original, claimed source (*e.g., Mackay, pg. 2, "look for the TTL value – if it is less than the value you are expecting, then the user is behind a NAT").*

Applicant's arguments on pages 18 – 19 thus are unpersuasive for the reasons given above.

5. Continuing through page 22, Applicant argues language addressed above appearing in independent claims, as well as the pending dependent claims. Applicant's arguments rely on the reasoning addressed above, and thus are unpersuasive for the reasons give above.

Information Disclosure Statement

6. The information disclosure statements filed 11/22/2010 and 09/01/2010 fail to comply with 37 CFR 1.98(a)(3) because the items referenced therin do not include a

concise explanation of their relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each publication listed that is not in the English language.

7. Furthermore, the information disclosure statement filed 09/01/2010 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. No copy has been provided on the Foreign Patent Document "JP-2005287071".

8. The information disclosure statements of 11/22/2010 and 09/01/2010 have been placed in the application file, but the information referred to therein has not been considered.

Claim Objections

9. Claim 33 is objected to because of the following informalities: said claim concludes with a comma rather than a period. Appropriate correction is required.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claim 39 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

12. Regarding claim 39, said claim recites on lines 8 - 9:

"*checking … whether a round-trip time ... is* ***significantly different***"

(emphasis added).

The precise meets and bounds of the language "significantly different" are unclear; i.e., it is unclear when a value would transition from being merely "different" to then having enough difference to be considered "significantly different".

13. In order to perform a complete examination, claim 39 has been interpreted broadly.

14. Claims 44 and 46 – 49 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 44, said claim is directed to:

"*A system, implemented at least in part in hardware … comprising:*

an information element receiver to receive information …

a feature discovery module to identify … and

a feature incompatibility analyzer … to determine"

The claim limitations "*receiver to receive*", "*module to identify"*, and "*analyzer … to determine"* use non-structural terms coupled with functional language (similar to "*means for*" limitations). It is unclear if applicant wishes to the have the claim limitations treated under 35 U.S.C. 112, sixth paragraph.

If applicant wishes to have the claim limitation treated under 35 U.S.C. 112, sixth paragraph, applicant may state so and amend the claim to include the phrase "means

for" or "step for". The phrase "means for" or "step for" must be modified by functional language, and the phrase or term must **not** be modified by sufficient structure, material, or acts for performing the claimed function. Furthermore, Applicant is reminded that if 35 U.S.C. 112, sixth paragraph, the structure referenced by the invoking claim language must clearly be expressly be recited by Applicant's Specification.

If applicant does **not** wish to have the claim limitation treated under 35 U.S.C. 112, sixth paragraph, applicant may amend the claim so that it will clearly not invoke 35 U.S.C. 112, sixth paragraph, or present a sufficient showing that the claim recites sufficient structure, material, or acts for performing the claimed function to preclude application of 35 U.S.C. 112, sixth paragraph.

15. Regarding claim 46 – 47, said claims recite further limitations regarding the system discussed above in claim 44, but fail to rectify the issues discussed above.

16. Regarding claim 48, said claim depends on above discussed claim 44, and further recites:

"*a parameter obtainer, for obtaining…*".

Said "*obtainer for obtaining*" suffers from the same indefiniteness under 35 U.S.C. 112 2nd paragraph, due to the ambiguity regarding invocation of 35 U.S.C. 112 6th paragraph, as was discussed above with regards to the limitations of claim 44. The logic applied to claim 44 thus similarly applied to claim 48.

17. Regarding claim 49, said claim depends on above discussed claim 44, and further recites:

"*a feature database for storing…*".

Said "*feature database for storing*" suffers from the same indefiniteness under 35 U.S.C. 112 2nd paragraph, due to the ambiguity regarding invocation of 35 U.S.C. 112 6th paragraph, as was discussed above with regards to the limitations of claim 44. The logic applied to claim 44 thus similarly applied to claim 49.

18. In order to perform a complete examination, the claims 44 and 46 – 49 have been interpreted broadly, and as not invoking 35 U.S.C. 112, sixth paragraph.

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. Claims 1 – 5, 9 – 20, 32, 38 and 43 – 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi (US 2003/0110274 A1) in view of Mackay (comp.os.ms-windows.networking.tcp-ip. "Can my ISP say if i'm using a proxy?" 2/16/2002. pgs. 1 - 4.).

21. Regarding claim 1, Pazi shows a method of making a determination, the method comprising:

receiving a communication from the potential device, the communication comprising a first information element (*e.g., a claimed source address, [7,15,30]*) and a second information element (*e.g., a TTL from the intercepted communication, [7,15,30]*)

wherein the potential device is an original source of said second information element;

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the packet, [30,47]*)

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*)

determining, using a detection system implemented at least in part in hardware, that the feature of the original source of said first information element and the feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]*),

said determining being indicative that the potential device is a device (*showing determining that a packets source is not what is claimed in an received packet and thus a potential bogus/hacker device is such a device; Figs. 2,3, [7-17, 30]*),

Pazi does not show where the determination is: whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing TTL values of received packets to detect the presence of devices*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify

and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

22. Regarding claim 2, Pazi in view of Mackay further show wherein said second information element is of a type that a relay device of a class of relay devices is unlikely to relay (*Mackay, pg. 2*).

23. Regarding claim 3, Pazi in view of Mackay further show wherein said class of relay devices is selected from the group consisting of a SOCKS proxy, an HTTP proxy using the GET method, an HTTP proxy using the CONNECT method, an IP router and a NAT device (*Mackay, pg. 2*).

24. Regarding claim 4, Pazi in view of Mackay further show wherein said second information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL (*Mackay, pg. 2*).

25. Regarding claim 5, Pazi in view of Mackay further show wherein said first information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL (*Mackay, pg. 2*).

26. Regarding claim 9, Pazi in view of Mackay further show wherein said stage of determining further comprises:

comparing said feature of an original source of said first information element with said feature of the potential relay device (*Pazi, [55]*).

27. Regarding claim 10, Pazi in view of Mackay further show obtaining a parameter indicative of said feature of an original source of said first information element; and

obtaining a parameter indicative of said feature of the potential relay device (*Pazi, [7-17] and Figs. 2, 3*).

28. Regarding claim 11, Pazi in view of Mackay further show wherein said stage of determining further comprises:

considering a time at which at least one of said feature of an original source of said first information element and said feature of the potential relay device, was discovered (*Pazi, [44]*).

29. Regarding claim 12, Pazi in view of Mackay further show obtaining a parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device (*Pazi, [44, 50-52]*).

30. Regarding claim 13, Pazi in view of Mackay further show wherein said stage of determining includes analyzing said parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device (*Pazi, [44, 50-52]*).

31. Regarding claim 14, Pazi in view of Mackay further show wherein said parameter is obtained from at least one of said first information element and said second information element (*Pazi, [44, 50-52]*).

32. Regarding claim 15, Pazi in view of Mackay further show c) sending an outgoing communication to at least one of said original source of said first information element and the potential relay device (*Pazi, [16]*); and

receiving a third information element from said at least one of said original source of said first information element and the potential relay device (*Pazi, [16-18]*).

33. Regarding claim 16, Pazi in view of Mackay further show e) deriving from said third information element information related to a feature of said at least one of said original source of said first information element and the potential relay device (*Pazi, [16-18, 44, 49-52]*).

34. Regarding claim 17, Pazi in view of Mackay further show verifying that an original source of said third information element is said original source of said first information element (*Pazi, [16-18, 47]*).

35. Regarding claim 18, Pazi in view of Mackay further show verifying that an original source of said third information element is the potential relay device (*Pazi, [54]*).

36. Regarding claim 19, Pazi in view of Mackay further show wherein said third information element is selected from the group consisting of an ICMP message, an ICMP Echo Reply message, a DNS query, an HTTP request, an HTTP response, an HTTP `Server` header, an IP address, a TCP port, a TCP Initial Sequence number, a TCP Initial Window, a WHOIS record, and a reverse DNS record (*Mackay, pg. 2 and Pazi, [60-62]*).

37. Regarding claim 20, Pazi in view of Mackay further show wherein at least one of said feature of an original source of said first information element and said feature of the potential relay device is a feature related to a configuration status (*Mackay, pg. 2*).

38. Regarding claim 32, Pazi in view of Mackay further show wherein at least one of said feature of an original source of said first information element and said feature of the

potential relay device is selected from the group consisting of a sub-network (*Pazi, [47,52*), an administrator, and a location (*Mackay, pgs. 1 – 2 and Pazi, [35]*).

39. Regarding claim 38, Pazi shows a method of making a determination, the method comprising:

receiving from the potential device a first information element (*e.g., a claimed source address, Pazi [7,15,30]*) and a second information element (*e.g., a TTL value, Pazi [7,15,30]*);

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the first information element packet, [30,47]*);

identifying a feature of an original source of the second information element (*identifying the TTL value in the currently received/incoming second information element packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*);

determining, using a detection system that the feature of an original source of said first information element and the feature of the original source of said second information element are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]*),

said determining being indicative that the potential device is a device (*showing determining that a packets source is not what is claimed in an received packet and thus a potential bogus/hacker device is such a device; Figs. 2,3, [7-17, 30]*),

Pazi does not show where the determination is: whether the potential device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing TTL values of received packets to detect the presence of devices*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

40. Regarding claim 43, Pazi shows a method of determining whether a potential device is a device, the method comprising:

identifying a feature of an original source of a first information element (*e.g., a claimed source address, [7,15,30]*);

identifying a feature of the potential device that transmitted the first information element and a second information element, the potential device being the original source of the second information element (*e.g., identifying a "authenticated", "reference" TTL value from the packet, [30,47], as well as identifying a TTL from the intercepted communication, [7,15,30]*); and

determining, using a detection system, whether a feature of an original source of a first information element and a feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs.*

2, 3, [14, 7-17, 23, 30, 67-68]),

wherein a positive result of said determining is indicative that the potential device is a device (*showing determining that a packets source is not what is claimed in an received packet and thus a potential bogus/hacker device is such a device; Figs. 2,3, [7-17, 30]*).

Pazi does not show where the determination is: whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing TTL values of received packets to detect the presence of devices*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

41. Regarding claim 44, Pazi shows a system, implemented at least in part in hardware, to determine whether a potential device is a device, the system comprising:

an information element receiver to receive information elements from a plurality of devices including an information source device and the potential device (*[7,15,30]*);

a feature discovery module to identify at least one of a feature of the information source device (*e.g., identifying the "authenticated", "reference" TTL value from the packet, [30,47]*) and a feature of the potential device (*e.g., identifying the TTL value in the currently received/incoming packet, which is then compared "against reference*

values" stored in the database of authentic, reference values [30,47,67]);

a feature incompatibility analyzer, using a feature database (Pazi, [9,30]), to determine whether thefeature of said information source device and the feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]*).

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (*pg. 2, describing utilizing TTL values of received packets to detect the presence of devices*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

42. Regarding claim 46, Pazi in view of Mackay further show wherein said information element receiver is further configured to receive information elements from a monitored host (*Pazi, [55-58,61]*).

43. Regarding claim 47, Pazi in view of Mackay further show an outgoing information element sender (*Pazi, [61]*).

44. Regarding claim 48, Pazi in view of Mackay further show a parameter obtainer, for obtaining at least one parameter selected from the group consisting of a parameter

indicative of a feature of an information source device, a parameter indicative of a feature of the potential relay device, and a parameter indicative of whether a feature of said information source device and a feature of said potential relay device are features unlikely to relate to a single device (*Pazi, Figs. 2 and 3, [52]*).

45. Regarding claim 49, Pazi in view of Mackay further show a feature database for storing a map between pairs of features and data indicative of whether said pairs of features are incompatible features (*Pazi, [47,54]*).

46. Regarding claim 50, Pazi shows a computer-readable non-transitory storage medium, comprising instructions, which when executed by a computer cause the computer to:

receive from the potential device a first information element (*e.g., a claimed source address, [7,15,30]*) and a second information element (*e.g., a claimed source address, [7,15,30]*) wherein the potential device is an original source of said second information element;

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the packet, [30,47]*)

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*)

determine whether the feature of an original source of said first information element and the feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a bogus/hacker device*

versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]),

wherein a positive result of said determining is indicative that the potential device is a device (*showing determining that a packets source is not what is claimed in an received packet and thus a potential bogus/hacker device is such a device; Figs. 2,3, [7-17, 30]*).

Pazi does not show where the determination is: whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing TTL values of received packets to detect the presence of devices*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

47. Claims 7 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Reed (Applying the OSI Seven Layer Network Model to Information Security. November 21, 2003).

48. Regarding claim 7, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not show wherein said first and said second

information elements are sent in two different layers of a protocol stack.

Reed shows wherein said first and said second information elements are sent in two different layers of a protocol stack (*Reed, pg. 24*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Reed in order to exploit common knowledge relating to networking and information security (Reed, pg. 1).

49. Regarding claim 33, Pazi in view of Mackay show claim 32.

Pazi in view of Mackay do not show wherein said determining includes examining a parameter indicative of at least one of said feature of a source of said first communication and said feature of a source of said second communication, and said parameter is selected from the group consisting of an HTTP `User-Agent` header, an RFC 822 `X-Mailer` header, an RFC 822 `Received` header, an RFC 822 `Date` Header, an IP address, a WHOIS record, and a reverse DNS record.

Reed shows wherein said determining includes examining a parameter indicative of at least one of said feature of a source of said first communication and said feature of a source of said second communication, and said parameter is selected from the group consisting of an HTTP `User-Agent` header, an RFC 822 `X-Mailer` header, an RFC 822 `Received` header, an RFC 822 `Date` Header, an IP address, a WHOIS record, and a reverse DNS record (*Reed, pgs. 23 – 24*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Reed in order to

exploit common knowledge relating to networking and information security (Reed, pg. 1).

50. Claims 21, 22, 23, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Nilsen (alt.comp.lang.php. "how to detect PROXY?" 12/24/2001. pgs. 1-2).

51. Regarding claim 21, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not show wherein said feature related to a configuration status is selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting and a time zone setting.

Nilsen shows wherein said feature related to a configuration status is selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting and a time zone setting (*pg. 1*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Nilsen more frequently be able to identify device types (*Nilsen, pg. 1*).

52. Regarding claim 22, Pazi in view of Mackay and Nilsen further show wherein said determining includes examining a parameter indicative of said feature related to a configuration status (*Nilsen, pg. 1*).

53. Regarding claim 23, Pazi in view of Mackay and Nilsen further show wherein said parameter is selected from the group consisting of an HTTP `User-Agent` header, an RFC 822 `X-Mailer` header, an RFC 822 `Received` header, an RFC 822 `Date` header, a protocol implementation manner, a TCP/IP stack fingerprint, an IP address, a TCP port, a TCP initial sequence number, a TCP initial window, a WHOIS record, and a reverse DNS record (*Mackay, pg. 2*)

54. Regarding claim 34, Pazi shows a method of determining whether a potential device is a device, the method comprising:

receiving from the potential device a first information element (*e.g., a claimed source address, [7,15,30]*) and a second information element (*e.g., a claimed source address, [7,15,30]*) wherein the potential device is an original source of said second information element

analyzing a configuration status of an original source of at least one of said first and said second information elements (*Pazi, [7-17]*)

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the packet, [30,47]*)

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*)

determining, using a detection system, whether the feature of an original source of said first information element and the feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are*

from a bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]).

Pazi does not show where the determination is: whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2*, *describing utilizing TTL values of received packets to detect the presence of devices*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

Pazi in view of Mackay do not show said configuration status selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting, and a time zone setting.

Nilsen shows said configuration status selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting, and a time zone setting (*pg. 1*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Nilsen more

frequently be able to identify device types (*Nilsen, pg. 1*).

55. Claims 24 – 31, 35,36 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Daude (US 6,892,235 B1).

56. Regarding claim 24, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not explicitly show wherein at least one of said feature of a source of said first information element and said feature of the potential relay device is a feature related to communication performance.

Daude shows wherein at least one of said feature of a source of said first information element and said feature of the potential relay device is a feature related to communication performance (*col. 7 lines 25 - 34, Figs. 5 – 7*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (*Daude, col. 7 lines 25 - 34*)

57. Regarding claim 25, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a measured communication performance, a measured relative communication performance, and an estimated communication performance (Daude, Figs. 5 – 7).

58. Regarding claim 26, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a latency of communication, a latency of an incoming communication, a latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate (Daude, col. 8 lines 36 – 40).

59. Regarding claim 27, Pazi in view of Mackay and Daude further show wherein said determining includes examining a parameter indicative of said feature related to communication performance (*Pazi, [34]*).

60. Regarding claim 28, Pazi in view of Mackay and Daude further show wherein said parameter is selected from the group consisting of time of receipt of an information element, time of sending of an information element, a round trip time, a round trip time gap, an IP address, a Whois record, a reverse DNS record, and a rate of acknowledged information (*Daude, col. 8 lines 36 – 40*).

61. Regarding claim 29, Pazi in view of Mackay and Daude further show wherein a higher round trip time gap is indicative of a higher likelihood that a relay device is being used for malicious purposes (*Daude, col. 8 lines 60 – 65*).

62. Regarding claim 30, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is estimated from information about at least one of said original source of said first communication and the potential relay device (Daude, Abstract).

63. Regarding claim 31, Pazi in view of Mackay and Daude further show wherein said information about at least one of said original source of said first communication and the potential relay device is selected from the group consisting of a location of a device, a reverse DNS record of a device's IP address, and an administrator of a device (*Daude, col. 11 lines 48 – 60*).

64. Regarding claim 35, Pazi shows a method of determining whether a potential device is a device, the method comprising:

receiving from the potential device a first information element (*e.g., a claimed source address, [7,15,30]*) and a second information element (*e.g., a claimed source address, [7,15,30]*) wherein the potential device is an original source of said second information element;

analyzing, using a detection system, a feature of an original source of at least one of said first and said second information elements (*e.g., identifying the "authenticated", "reference" TTL value from the packet, [30,47]*);

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the packet, [30,47]*);

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*);

determining, using a detection system, whether a feature of an original source of said first information element and a feature of the potential device are features unlikely to relate to a single device (*showing determining when communications are from a*

bogus/hacker device versus when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]),

Pazi does not show where the determination is: whether the potential device is a relay device and where said detection system is a relay detection system.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2*, *describing utilizing TTL values of received packets to detect the presence of devices*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

Pazi in view of Mackay do not show b) analyzing a feature related to communication performance of an original source of at least one of said first and said second information elements.

Daude shows analyzing a feature related to communication performance of an original source of at least one of said first and said second information elements (*col. 7 lines 25 – 34, Figs. 5 – 7*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (*Daude, col. 7 lines 25 – 34*).

65. Regarding claim 36, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a latency of communication, a latency of an incoming communication, a latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate (*Daude, col. 8 lines 36 – 40*).

66. Regarding claim 39, Pazi shows method of determining whether a potential device is a device, the method comprising:

receiving from the potential device a first information element (*e.g., a claimed source address, [7,15,30]*) and a second information element (*e.g., a claimed source address, [7,15,30]*) wherein the potential device is an original source of said second information element;

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the packet, [30,47]*)

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*); and

checking, using a detection system, whether an element of the address of the potential relay device is significantly different than an element of the address of the original source of said first information element (*showing determining when communications are from a bogus/hacker device versus when communications are from*

an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]; said determination performed using values of the currently received/incoming packet, which are then compared "against reference values" stored in the database of authentic, reference values [30,47,67]).

Pazi does not show where the determination is: whether the potential device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing TTL values of received packets to detect the presence of devices*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

Pazi in view of Mackay do not show checking round-trip times.

Daude shows checking round-trip times (*Figs. 1, 4, 6 and col. 8 lines 25 – 65*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (*Daude, col. 7 lines 24 - 35*).

67. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over (US 2003/0070096 A1), hereafter Pazi2 (where Pazi, US 2003/0110274 is incorporated by reference into Pazi2 in Pazi2, [1]) in view of Mackay.

68. Regarding claim 37, Pazi2 shows a method of determining whether a potential device is a device, the method comprising:

sending a message to an information source device, triggering said information source device to send a DNS request to a DNS server (*Pazi2, Fig. 2 items 42 and 44*)

monitoring said DNS request from said information source device to said DNS server (*Pazi2, item 46*)

identifying a feature of an original source of the first information element (*Pazi,* describing *identifying "authenticated", "reference" TTL values, [30,47], where said values can be verified/derived from DNS requests, [63]*)

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*)

determining, using a detection system, based on the feature of the information source device and the feature of the potential device whether said potential device is a device (*Pazi2, items 48 – 52 and [18-19]*).

Pazi2 does not show where the determination is: whether the potential device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing TTL values of received*

packets to detect the presence of devices).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

69. Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay and Augart (US 7,200,673 B1).

Regarding claim 41, Pazi shows a method of making a determination, the method comprising:

receiving, from the potential device, a first information element (*e.g., a claimed source address, [7,15,30]*) and a second information element (*e.g., a claimed source address, [7,15,30]*) wherein the potential device is an original source of said second information element;

identifying a feature of an original source of the first information element (*identifying the "authenticated", "reference" TTL value from the packet, [30,47]*)

identifying a feature of the potential device (*identifying the TTL value in the currently received/incoming packet, which is then compared "against reference values" stored in the database of authentic, reference values [30,47,67]*)

checking, using a detection system, whether the feature of potential relay device is different than the feature of an original source of said first information element (*showing determining when communications are from a bogus/hacker device versus*

when communications are from an authentic device; Figs. 2, 3, [14, 7-17, 23, 30, 67-68]).

Pazi does not show where said identified feature is a location.

Augart shows where said identified feature is a location (*col. 4 line 56 - col. 5 line 20, col. 10 lines 11 - 47*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the TTL comparison disclosure of Pazi with the TTL comparison teachings of Augart in order to utilize available information to derive additional network informaiton, allowing quick identification of devices, aiding in network problem diagnosis, as well as assisting in surveys and research (*Augart, col. 4 lines 55 – 60 , col. 12 lines 50 - 60*).

Pazi in view of Augart do not show where the determination is: whether the potential device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device using a relay detection system (*pg. 2, describing utilizing TTL values of received packets to detect the presence of devices*).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Augart with that of Mackay in order to best identify and understand the actual sources of received traffic and thus better control the types of traffic admitted to your network (*Mackay, pgs. 1 - 2 and Pazi, [3-9]*).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. MacIlwinen whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenn Burgess, can be reached on (571) 272 - 3949. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JOHN MACILWINEN/
Examiner, Art Unit 2442

(571) 272 - 9686